Number 3-97

security awareness bulletin

Inside

Risk Management

Risk Management and Security Education.....1
Challenges of Risk Management.....3
5 Steps to Better Risk Management Decisions 5
Measuring Risk.....17
Analytical Risk Management 23
Training for Risk Management.....27
Summary of Changes to 5200.1 and 5200.1-R 35

plus more

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publicaiton Reproduction authorized except where noted

September 1997

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

The Security Awareness Bulletin is produced by the Department of Defense Security Institute, Richmond, Virginia. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and education methods.

For new distribution or address changes:

- Air Force: Contact your local Publication Distribution Office. Ask for "DODSISAB."
- Army, Navy, Marine Corps, and Department of Defense agencies: DoD Security Institute, Attn: SEAT, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091, POC Tracy Gulledge, (804) 279-4223, DSN 695-4223; fax (804) 279-6406, DSN 695-6406. E-Mail gulledget@dodsi.dscr.dla.mil
- For other government agencies and contractors, you can order this publication through the Government Printing Office (see page 43), or download it from the Internet. Our URL is http://www.dtic.mil/dodsi.

Risk Management and Security Education

A note to the Security Educator:

Risk management has been proclaimed to be the guiding philosophy of modern security programs. According to Gail Howell in our introductory article, "It is going to be our new way of doing business and will be with us for years to come." Risk management stands in contrast to risk avoidance, how we addressed security in the past, which was doing everything possible to prevent loss or damage without reference to the degree of risk. The new philosophy offers a rational and defendable method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valued assets. Through risk management we should be able to answer the question, often left unanswered in the past: **"How much security is enough?"**

Seasoned professionals will argue, however, that this is no radical revolution. In reality, they have made and still make common-sense judgment calls when time and resources are limited. But the methodology of risk management calls for a more deliberate, systematic approach to decision-making than the educated guess. Risk management dictates that we do only those things which are justified as the result of *a systematic assessment of the degree of risk* in a situation.

The following articles by Gail Howell, Ed Jopeck, Aimee Hummel, and Richards Heuer discuss risk management philosophy and practice from a variety of perspectives in government. Ed Jopeck's contribution, in particular, demonstrates how to apply the method in a practical situation. By following a five-step process we can make risk management decisions about how much and what kind of security to put in place. It requires measurement, estimation, and careful judgment based on the available data. And, as pointed out by Gail Howell, risk management puts tremendous pressure on the security professional. He or she must present a convincing and a clear analysis to sell the "countermeasures approach" to asset owners.

Decision-making about security is now more complicated and many of us would benefit from basic training on this subject. This issue, in fact, concludes with an overview of risk management training provided by several agencies including the DoD Security Institute and the dates of future courses.

Risk Management as applied to Security Awareness:

If the adoption of risk-management principles in the overall conduct of security programs tell us how much and what kind of security is enough, the same should tell the security educator ***how much security education is enough*** for our employee populations. After all, the enhancement of security awareness is an extremely important security countermeasure.

And you as an educator are a prime candidate for embracing a more systematic approach to decision-making and the allocation of scarce resources. There are a number of reasons for this. Historically, while budgets have been limited, security educators have had an austere discretionary freedom to get the job done. Minimum standards about how to conduct security awareness programs are increasingly open to interpretation. And budgets are often negotiable with management (when management is on our side). We have had to make tough decisions and, in an unsystematic way, have followed the principle of placing the resources where they are needed most. One type of decision

has been about the choice of media and delivery systems for getting the message across.

Consider what a security educator might want to know in order to follow a five-step risk-management strategy for carrying out an effective security awareness program:

- the value of what we are trying to protect, and the consequences of its loss to national security.
- the magnitude of the foreign intelligence threat (or other type of threat) at our physical location.
- the probability of inadvertent loss of sensitive information where employees lack sufficient knowledge of safeguarding rules and procedures.
- the human vulnerabilities of our employees—their behaviors, attitudes, and current awareness.
- whether these people know how to use countermeasures selected by management.
- the cost of everything we do to deliver the message—comparing the tradeoffs between CD ROM briefings, posters, newsletters, live briefing programs, CBT, etc.

Admittedly, in all of this there is the problem of measurement and making valid estimates. But the objective is to make decisions about our educational programs that can be justified in terms of the risks involved and the consequences of inaction. A convincing and clear analysis of what we do (and why) to enhance the awareness of our employee populations will gain management support.

The Challenges of Risk Management

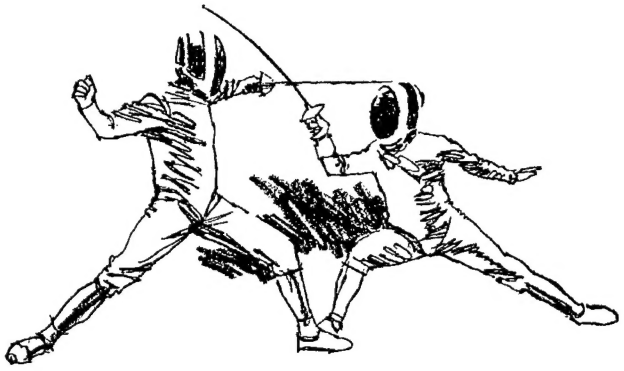
BY GAIL S. HOWELL
DEFENSE INTELLIGENCE AGENCY

It is one of the perennial misfortunes that good concepts acquire catchy names used so often that the underlying concept is lost. One hopes that confusion around the term "risk management" similarly does not lead to it becoming a hollow buzzword. Unfortunately, the term itself is confusing. If one accepts the term "risk" as defined in the dictionary—danger—one realizes that risk, like danger, is not managed. Rather, one hopes to prevent danger; to obviate risk. The methodology for risk management is still being solidified, so any thoughts below cannot be viewed as doctrine. The purpose of this piece is to portray the challenges to the security professional trying to cope with risk management.

One often encounters the term "risk management" as a contrasting phrase with "total risk avoidance." The new security world does risk management rather than total risk avoidance. The intent of the contrast is to show that flexibility now exists in the way security countermeasures are employed which heretofore did not. This charge of past inflexibility tends to put security professionals on the defensive because it implies that a realistic, commonsense approach toward security did not exist in the past. A lot of consumers would concur with that assessment. Security was rule bound. "You can't do that" was the operant phrase. However, there was a reason for this approach to security.

A rule-based world is an easy one for security professionals. You set the standards and force people to follow the rules. If they don't, you give them a ticket, AKA a security violation. However, people (spies and non-spies alike) are pretty resourceful and find ways around rules. The non-spies don't necessarily do it maliciously, but because they view the rules as hindering efficiency.

A rule-based world is easy for the trainer. One teaches the rules. One does not necessarily even have to explain the basis for the rules. Students often want a primer, not a range of options. In the risk management world, students will have to understand the rationale for why certain countermeasures are employed and how to assess what is the right mix of security techniques for a given situation. Risk management



implies a holistic approach toward security, where one looks at the entire range of security countermeasures (encompassing personnel, physical, technical, computer, and information security) and how they interact to protect a site or organization.

At this point the reader is probably saying, "All right already, just give me the definition." There are many variants, but for purposes of this article, risk management is a process that consists of five parts:

- An assessment of the value of an asset
- Identification of the threat to that asset
- Definition of the vulnerabilities of the asset
- Identification of security countermeasures that could nullify/reduce the threat to the asset.
- Analysis of the cost/benefits of employing the countermeasures

The above process presents many challenges to security professionals. Perhaps taking a look at each of the above steps will give some insight into the magnitude of the challenge.

A security professional cannot judge the value of an asset. Only the owner of the asset can provide an assessment of its value. It may prove difficult, however, to elicit such a statement. The method for doing so is not straightforward. For example, the new Director of Central Intelligence guidelines on physical security of sensitive compartmented information facilities require inspection frequency to be based on threat, the value of the information at the facility, past

security performance and major changes occurring in a structure. Clearly, risk management philosophy has been applied to these guidelines. However, the method for determining the value of the information in facilities has not been established.

In the past, security professionals treated all facilities alike. The value of the information or asset was its classification. Risk management implies that some things classified Secret are more important than other things classified Secret even though they all meet the national security criteria for Secret classification. One starting point for those planning the inspection of facilities will be to meet with the program managers for Defense critical technologies and learn which facilities are involved in research, development and testing. This is based on the assumption that critical technologies are of great interest to spies. Which brings us to threat.

Traditionally, many rules for employing security countermeasures were based on worst case scenarios. Once the rules were established, security professionals did not have to explain the underlying rationale for the rules. This meant that security professionals could be quite successful by knowing the rules. They did not need a detailed knowledge of threat. Nor did they clamor for collection of detailed threat information.

The security world has changed since the end of the Cold War. Instead of devising countermeasures to a monolithic threat, the security community is being asked to address the threat against each site or asset—clearly a challenging task. To do this, each security professional must be armed with available threat information when devising a countermeasure strategy for a consumer. With the establishment of the National Counterintelligence Center, the security community has a unique opportunity to express its requirements for detailed threat information.

The risk management processes of identifying asset vulnerability and potential countermeasures to reduce vulnerability should be relatively straightforward. The greatest challenge in this area is being posed to computer security professionals who are continually in a race to stay current on the latest techniques for countering hackers and viruses. One must also not forget the challenges posed by enemies within, as evidenced by the recent Ames case.

The most "emotional" issue for security professionals will be the new emphasis on cost benefit analysis required by risk management. Cost was not a driving issue in the past. Security professionals aimed for the best security countermeasures against the worst case threat. Now a range of options and their cost must be presented to the consumer. Security professionals should not feel left at sea in this regard. As mentioned above, it would be impossible, given the number of classified sites around the world, to take a totally site-based approach to employing security countermeasures. Standards will continue to exist to provide a baseline of security countermeasures. These can be waived after a risk management assessment occurs of a given site or asset.

In fact, so pervasive is the view that security has taken an overkill approach in the past, some recent standards require notification of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence or the Director of Central Intelligence when the standards are exceeded. A number of new security standards have recently been written; several are in revision. It is important that security professionals keep up with the changes, and re-educate themselves.

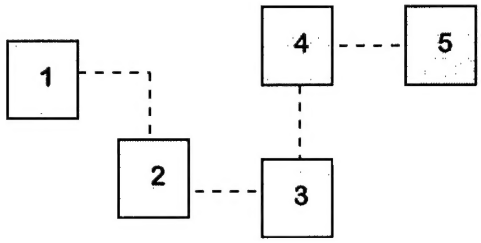
The assumption of risk is a decision that the owner of the asset must make based on the recommendations of the security professional. The security professional becomes a persuader rather than a regulator. There are still approval procedures in place that will prevent wanton disregard of security by asset owners. The difference is that a risk management approach gives them voice, allows them to have an impact on which security measures are employed.

Risk management puts tremendous pressure on the security professional. He or she must present a convincing and clear analysis to sell the countermeasures approach. Expertise will be key to success. These challenges may seem daunting to security professionals, but actually they should be viewed as exciting. Flexibility allows for creativity. This in turn leads to professional growth. Security professionals need to embrace these challenges and devise new ways of approaching security support to consumers. Risk management is not going to become another empty phrase. It is the new way of doing business and will be with us for years to come.

Ms. Howell is the chief of the Security Division in the Office for Security and Counterintelligence, Defense Intelligence Agency.

The Risk Assessment:

Five Steps to Better Risk Management Decisions



BY EDWARD J. JOPECK

The author is a member of the risk management working group under the U.S. security policy board and a member of the analytical risk management training development team, which was recently awarded a national intelligence citation by the Director of Central Intelligence.

Since the Joint Security Commission published its report on reinventing government security in 1994, we all have been hearing a great deal about **risk management**. If you ask any security professional they can probably tell you that it is a *new security process based on sound threat analysis and risk management practices*. They may even tell you that risk management will provide the U.S. Government *the security it needs at a price it can afford*. But if you ask them *how* to conduct a risk analysis, you are less likely to get a concise answer. Likewise, despite its importance to the risk management process, examples of risk assessments are still surprisingly difficult to find. It is easy to conclude from such experiences that the theory of risk management is well known, but genuine understanding and use of the risk analysis in security decision making remains elusive.

It is now mid-1997 and a national policy requiring the use of risk management in government security decision-making is rumored to be just around the corner. The policy will most likely require that government and industry security professionals use a structured and consistent risk analysis to support their security decisions. If this is the case, the new and urgent business at hand for many in the security field is to learn how to conduct the risk assessment, the process which provides the very foundation for risk management decision making. Likewise, senior security managers and decision makers would be wise to consider how the risk assessment process is likely to change the way they are expected to make security decisions.

Although experience has shown the theory of risk management makes good, even "common" sense, its use in the imperfect world of reduced budgets and highly bureaucratic organizations comes with some potential pitfalls which managers and decision makers will want to avoid. The potential to be caught off-guard by these errors – the kind of errors that can come with serious consequences to National Security and human life – could be far greater when security professionals with only a modest understanding of the risk management process begin their first unguided steps toward its implementation.

In an effort to ease the transition from the theoretical to the practical application of risk management, this article shows the practical use of the risk assessment in the process of risk management for those security professionals who lack the time or opportunity to learn the process in a classroom setting. It will take the reader through a simplified risk assessment and discuss the benefits and pitfalls of which analysts, practitioners, supervisors, and decision makers should be aware. [1]

The Risk Analysis

The risk management process encapsulates two key components: a structured risk analysis which determines the existing and recommended levels of risk, and a decision by a *decision maker*, which determines what will be done about those risks.[2] Since the decision is expected to be based on the assessment of risk, the two components should oc-

[1] The charts and ratings used here should not be interpreted as representative of an actual analysis, as more complex charts, spreadsheets and research are normally used in the analytical process.

[2] Although not all security professionals consider themselves analysts, the term is used here to denote anyone who conducts a risk analysis.

cur in sequence starting with the risk analysis. Additionally, the risk analysis is sometimes followed by a cost-benefit analysis. The risk analysis, and cost benefit analysis when applicable, then form the analytical structure on which the decision maker may ultimately base their risk management decisions.

In order to discuss the risk analysis, it is useful to begin with a common understanding of what constitutes an "analysis." The common definition of an "analysis" is *the process of breaking the whole of something into its component parts for further study*. Similarly, the analysis of risk can be defined as *breaking-down a security issue into the components of risk for further study*. In security analysis, these components are assets, threats, vulnerabilities, and countermeasures. Each of these components can also be broken down again, repeating the process as necessary to develop and document the differences between the what is being studied.

Laying the Foundation for a Sound Analysis

Before beginning any analysis, some time should always be spent in clarifying the tasking and preparing for the study. When possible, an interview or brief conversation with the requester will help the analyst confirm why the study is needed. Knowing this will help in defining the scope of the study and may also help identify the most likely sources of useful information. Without such preparation, the analyst's initial research will likely result in the collection of too much extraneous and irrelevant information. Should this happen, the research may become unfocused and its results difficult to manage.

Since analysis is most useful when it is objective, an examination of the likely objectivity of each study should also take place during the preparation stage. Prior to beginning a study, the analyst should give careful consideration to any feelings or conflicts they, or others may have. Both the analyst and the manager should be wary of strong expectations or pressures regarding the outcome of the analysis if they are not based on asset, threat, or vulnerability information. The most common of these external pressures – budgetary and political constraints – are valid factors for the manager and should be considered within the context of the risk management decision, but they should play no role in determining the outcome of the risk analysis.

Definitions of Risk Management Terms used in this Article

Risk assessment is the process of evaluating threats to, and vulnerabilities of, an asset to give an expert judgment on the probability of loss or damage, with the impact of loss as a guide to taking action.

Cost benefit analysis is the part of the management decision-making process in which the costs and benefits of each alternative are compared and the most appropriate alternative is selected. Costs include not only the costs of equipment, but also the on-going operational costs associated with countermeasure implementation. Benefits are expressed in terms of the amount of risk reduction.

Decision maker: a person with the authority and resources to implement security countermeasures.

Asset is any person, facility, material, information, or activity which has positive value and requires protection. The asset may also have value to an adversary, although the nature and magnitude of those values may differ

Asset manager: A person who supervises, oversees, operates or controls assets on behalf of the U.S. Government.

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage to an asset. It can also be defined as the intent or capability of an adversary to undertake actions that would be detrimental to the asset owner's interests.

Adversary is an individual, group, organization, or government that conducts activities, or has the intent and capability to conduct activities detrimental to the assets of the asset owner.

Vulnerability can be defined as any weakness that can be exploited by an adversary to gain access or information from an asset. Vulnerabilities can result from, but are not limited to, building characteristics, equipment properties, personal behavior, operational practices.

Conducting the Analysis

Step 1: Asset Assessment

The logical first step in a typical risk analysis is the asset assessment. The asset assessment helps

Worksheet 1 – ASSET ASSESSMENT

Assets	Undesirable Events	Loss Impact Assessed as:
People	Injury or death(s) due to violent crime	critical
	Injury or death due to natural disaster or accident	critical
Residential Structure and Real Property	Damage or destruction due to hurricane/high winds	medium
	Flood damage/destruction	medium
	Fire damage/destruction	medium
	Vandalism damage	very low
Family Heirlooms and Photos	Loss or destruction by natural disaster, theft or vandalism	medium
Personal Property	Loss of property due to theft	low
	Loss of property due to vandalism	low

the risk management practitioner to identify and focus only on those critical assets that are worthy of protection. By identifying and trying to prioritize these assets, the practitioner is taking the first step in focusing their resources specifically on that which is most important to the US national security and to the organization.

The first thing we need to know about assets is what they are. Assets are most easily identified in categories. Although most asset categories, like people, buildings and computers are tangible, some, like anonymity of sources, operational readiness, or strategic advantage, are intangible. Although it is tempting for the analyst to identify these assets themselves, this information is best collected during interviews with program managers, facilities managers, computer systems managers and operational elements who are most familiar with them. (For the purposes of risk management analyses, we can call these individuals "asset managers.")

Through discussion with the asset manager (and other experts, when available) we can get their impressions of what the expected consequences would be if each individual asset was lost, harmed, or otherwise adversely affected. Using this information we can then rank the assets in order of the consequence of their loss, thus focusing on the assets in descending order of importance. By doing this we get both an understand of what could happen if the asset was lost, destroyed or otherwise neutralized, and a perspective on where it fits relative to other assets which should be protected.

Also included in the asset assessment is the identification of undesirable events. Since the unwanted event is the focal point of the entire risk analysis, we document each event which could adversely affect a specific asset, arranging them next to the asset(s) to which they correspond. Common unwanted events in government assessments include unauthorized entry, terrorist bombing, unauthorized access to sensitive computer files, and loss of classified documents, to name just a few.

Ideally, the result of the asset assessment will be a worksheet (as shown above) that identifies and organizes the key components of the assessment and their relationship to one another. Without such a worksheet, it will become difficult, if not impossible, to manage and interpret the mass of information that the analyst will gather during the subsequent research and interviews. (For demonstration purposes a sample worksheet is included in each section in this article, and a final chart is included at the end. The reader is encouraged to refer

to the corresponding worksheets, and the final chart as each step of the process is discussed.)

For the example used in this article, we will conduct a risk analysis on a simple residential property. This fictional property sits in an area subject to common crime, and occasional natural disasters. Since people and personal property are also resident at that location, they should also be included in the assessment. During the interview the fictional owner told the analyst that the safety and security of his family living in the residence is his primary concern. With the exception of family heirlooms and photographs, the owner feels everything else is either insured and/or easily replaceable. However, he feels his family heirlooms and family photos cannot be replaced and their loss would be a serious loss to the family history. Through the interview the owner has given us useful information about the problems with crime and weather-related damage he and others in the area have encountered in the past. These concerns provide the foundation for our unwanted events. Given this information we are able to draft a simple asset worksheet as follows:

Caution: *In rating the consequences of loss for assets in any part of the federal government it is important not to confuse the perspective of the asset manager with the asset owner. In many cases an asset may be important to an asset manager, agency or department, but may be of only minor importance to the U.S. Government, which ultimately owns it and pays for its security. Accepting an asset manager's assertion that an asset is critical, is to also assert it is critical to the U.S. Government. This is less frequently true, and could result in overprotection of an asset at the expense of more critical assets elsewhere.*

Step 2: Threat Assessment

The second step in conducting a risk analysis is the threat assessment. This step helps the risk management practitioner to focus attention specifically on which adversaries or events adversely affect the previously identified assets. It also presents the greatest challenge to security professionals who are unfamiliar with conducting in-depth intelligence research because it replaces the acceptance of intuition with a reliance on data and information obtained from research and interviews.

Threats are generally considered in terms of adversaries. Common examples are terrorists, criminals, foreign intelligence services, and so on. To know if an adversary poses a threat requires information about their capabilities, intent, and their history of attacking the assets listed in Step 1 of the assessment. (Natural disasters and accidents can also be included in undesirable events, although they do not possess intent.)

When it is known that an adversary has the intent and capability to attack a specific asset, this information is relied upon to assess the current threat level. However, when such information is unknown or unknowable (as is the case with natural disasters and accidents), the analyst must rely more on historical data, the judgment of experts, statistical probability, or occasionally assumptions[3] to help qualify and quantify the threat.

Threat data comes in many forms and from many different sources. Depending on the threat topic being researched, the best sources for a given threat can range from the Internet to Top Secret intelligence reporting. Unfortunately, many analysts overlook unclassified sources, even when they are likely to contain the best threat data. A good rule of thumb for deciding where to seek threat information is to determine if there are any businesses, professional or special interest groups concerned about the same threats (hackers, workplace violence, telephone fraud, for example). If so, there is an excellent chance valuable information will be available outside of classified sources. However, if the threat concerns the intelligence activities or sources and methods of the United States or other countries, chances are that the best threat information will be found only in classified sources.

In continuing with our earlier example, we note that the majority of our threats to this residence are criminal in nature. A likely research approach would be to start with the FBI's Uniform Crime

[3] Assumptions should be documented in the text or appendix of the written assessment.

Worksheet 2 – THREAT ASSESSMENT

Assets	Undesirable Events	Adversary	Intent	Capability[4]	History	Threat Level
People	Injury or death(s) due to violent crime	Violent criminals	yes – but target selection arbitrary	yes	very infrequent	low
	Injury or death due to natural disaster or accident	Flood, fire, hurricane, high winds, accident	N/A	yes – very random assessed as low	serious weather deaths occur every 2 to 3 years	low
Residential Structure and Real Property	Damage or destruction due to hurricane/high winds	Hurricanes/high winds	N/A	yes	extremely infrequent	very low
	Flood damage/destruction	nearby river	N/A	yes	frequent overflows	medium
	Fire damage/destruction	Electrical or stove fire, accident	N/A	yes	infrequent	low
	Vandalism damage	Vandals	yes – but target selection arbitrary	yes	infrequent	low
Family Heirlooms and Photos	Loss or destruction by natural disaster, theft or vandalism	Flood, fire, hurricane, high winds, vandals	N/A or arbitrary target selection	yes	infrequent	low
Personal Property	Loss of property due to theft	Burglars, petty thieves	yes – but target selection arbitrary	yes	common	medium
	Damage to property from vandalism	Vandals	yes – but target selection arbitrary	yes	infrequent	low

Reporting statistics and follow-up with an interview with the law enforcement agency with jurisdiction in the area. From our research we find there have been both violent and non-violent crimes reported recently in our area. Because these are mostly crimes of opportunity and have been committed by individuals acting alone, it is virtually impossible to quantify the intent of these potential criminals. Nevertheless, we can determine from the statistics that there is a history of this type of crime and that individuals acting alone clearly possess the capability to commit these simple crimes.

For the weather-related threats, we research some weather reporting sources on the Internet and complete the research with a search of press articles covering weather-related stories in our area. We determine that some weather-related damage has occurred in this area in the past. Flooding is a problem about once a decade. Violent weather patterns, however, are very infrequent. Although they sometimes cause property damage, they rarely result in severe injuries or death.

By using another worksheet (above) that lists assets and events from worksheet #1, threat assessment information can be efficiently organized, documented and later integrated into the complete analysis.

Step 3: Vulnerability Assessment

The third step in a typical risk analysis is the vulnerability assessment. The vulnerability assessment is familiar to most security professionals because it encompasses the traditional security survey. In this step, the analyst is looking for exploitable situations created by lack of adequate security, personal behavior, commercial construction techniques and insufficient security procedures. Typical vulnerabilities can be phrased as weak door

[4] Capabilities used for this example are all very simple occurrences or criminal acts and hence the capability exists in all cases. When used in a real scenario, adversaries which have the ability to undertake attacks requiring advanced technical capabilities are less frequent.

locks, absence of guards, poor password controls, minimal setback of a building from the street, and so on.

The vulnerability assessment can also be an interesting exercise because it requires the analyst to look at an asset as each of the listed adversaries might look at it. Specifically, the analyst should begin by studying the asset and asking the question (or asking other subject matter experts): "If I were a petty thief, I would break into this house by..." or,

"If I wanted to physically harm the owner of this house I would..." and so on down the list of adversaries and unwanted events. Each vulnerability, when considered against the adversaries who might exploit them, and the assets they seek to attack, will then increase or decrease in importance, thus highlighting the relevant vulnerabilities most likely to be identified and exploited by the adversary.

As the analyst will notice, many risk assessments they will be asked to conduct will involve assets which already have some type of security countermeasures used to protect them. Although it may be tempting to accept these countermeasures as a valid starting point for the vulnerability analysis, it should be recognized that there are trade-offs for doing so. For example, not all of the existing countermeasures may still be necessary, nor are they necessarily still effective against rapidly-changing threats. Depending on the circumstances of the analysis this may, or may not, present a problem. Consequently, two types of vulnerability assessment approaches are discussed here.

The progressive analysis: The simplest way to evaluate existing countermeasures is to use the progressive analysis of countermeasures. To use this technique, the analyst simply determines how the existing countermeasures stack-up against the existing vulnerabilities. Although this gives the analyst a realistic picture of the current situation, it is not especially useful for evaluating the *optimum* countermeasures (in terms of efficacy and cost) or eliminating unneeded countermeasures. If using this technique, the analyst should be mindful that the existing countermeasures may have been recommended and implemented at a different time, with different threats in mind, and/or with different assets to protect. This technique can also make it more difficult to add future countermeasures, as issues of compatibility and continuation of the earlier security strategy can limit the number of options available for future countermeasures. When this is the case, security countermeasures packages can become increasingly dependent on outdated and ineffective countermeasures even though more effective, but incompatible, countermeasures are available.

The regressive analysis: A better way of evaluating assets with existing countermeasures is to perform a regressive countermeasures analysis. Simply stated, this process allows the analyst to assess the asset as if it was in a pure, unprotected state. After rating the vulnerability without the existing assets, the asset is then reevaluated taking into consideration the existing countermeasures. The differences between the unprotected and protected ratings represent the efficacy of the existing countermeasures. Ineffective countermeasures can then be identified and can later be recommended for elimination to achieve cost savings or to reallocate those savings to more effective countermeasures.

Although the regression analysis technique requires a little more work, it is better suited to assessments where an existing countermeasure or security program is being studied for elimination or reduction in resources. The result is a clearer comparison of each countermeasure and the benefit it provides in reducing the vulnerability to the asset or assets. This information can be very useful to managers in the task of balancing countermeasures options against budgetary constraints.

Vulnerability information is obtained from a variety of sources. A good starting place is always the people who work most closely with protecting the asset. For example, security guards almost always recognize vulnerabilities in their existing countermeasures either through past experiences or careful evaluation of their surroundings. Likewise, computer system administrators and program managers are likely to be aware of vulnerabilities in their systems through a variety of experience, professional publications, conferences and contacts. Often these professionals will highlight additional

vulnerabilities that require further study to determine if a threat with the intent, history or capability of exploiting vulnerability even exists.

To continue with our earlier example, let's assume our interview with the owner of our residence and our own security survey have revealed the following information:

- The house is in a subdivision near the river and has a robust neighborhood watch program.
- It was not designed with security in mind, however, and has weak locks on the doors and windows, and an unfenced yard with no garage.
- Because it is an old house, the electrical wiring is brittle and some of the structural members supporting the roof are in need of additional support.
- The last owner added some safety enhancements, like motion activated exterior lighting, smoke detectors, and fire extinguishers.

Upon obtaining and reviewing this information we can record our vulnerability assessment as shown in Worksheet #3. (For this example, we will use the progressive analysis technique.)

Step 4: Risk Assessment

The risk assessment is the step when all of the

Worksheet 3 – VULNERABILITY ASSESSMENT

Assets	Undesirable Events	Vulnerabilities	Existing Countermeasures	Vulnerability Level
People	Injury or death(s) due to violent crime	poor security habits, unprotected outside residence, weak locks	Door locks, alarm system	medium
	Injury or death due to natural disaster or accident	house on flood plain & poorly constructed, emergency response 20 miles away	basement for shelter, 911 preset on telephone, first aid kit in house	low-medium
Residential Structure and Real Property	Damage/destruction from hurricane/high winds	house is poorly constructed, many large trees in area	homeowner insurance	very low
	Flood damage/destruction	development constructed on flood plain, no water pump	flood insurance	medium
	Fire damage/destruction	old electrical wiring and appliances, emergency response 20 miles away	smoke detectors (2), fire extinguishers (2), homeowner insurance	medium
	Vandalism damage	exterior of house and cars unprotected	exterior lighting, neighborhood watch	medium
Family Heirlooms and Photos	Loss or destruction by natural disaster, theft or vandalism	house on flood plain & poorly constructed, emergency response 20 miles away, weak locks	Door locks, alarm system, exterior lighting, neighborhood watch	medium
Personal Property	Loss of property due to theft	weak locks, emergency response 20 miles away	Door locks, alarm system, exterior lighting, neighborhood watch	medium
	Damage to property from vandalism	exterior of house and cars unprotected	exterior lighting, neighborhood watch	medium

earlier assessments (asset, threat, and vulnerability) are combined and studied together to give a complete picture of the risks to an asset or group of assets. Using the worksheets in steps 1-3 the analyst has systematically analyzed the following questions:

- What is the likely impact if an identified asset is lost or harmed by one of the identified unwanted events?
- How likely is it that an adversary or adversaries can and will attack those identified assets?
- What are the most likely vulnerabilities that the adversary or adversaries will use to target the identified assets?

Assessing each of these questions has prompted the analyst to collect, study, and summarize the data into a brief rating. Now it is time to evaluate how each of the answers to those questions interact to increase or decrease risks. At this stage a final worksheet is extremely helpful in aligning all of this information into a readable and easily understood format which summarizes all of the previously collected information. Using the risk analysis worksheet #4 on page 10 as a guide, the analyst should, reading from left to right, review all of the important factors associated with that single asset, referring back to the earlier worksheets and supporting data when necessary to understand how each increases or decreases the overall risk. By reviewing these ratings, the analyst can finally begin to make an informed judgment on how "at risk" each of the assets is from its corresponding unwanted events.

The resulting conclusions of this analysis can then be summarized into a risk statement, linguistic or numerical rating.[5]

For example, the risk of damage to the residence or property in our example may be summarized into a concise risk statement:

The risk that the owner will suffer a serious loss from vandalism to the residential structure and real property is very low. Given the minimal value of the assets typically at risk in such a crime, the impact of an act of vandalism is assessed as very low. Likewise, the threat of individuals or groups seeking to vandalize this property is also deemed to be low. Although the residence itself is a moderately vulnerable target for such attacks, the existing countermeasures make the target less attractive to the common vandal. Finally, the owner's insurance coverage further mitigates any financial impact the owner could suffer from losses due to vandalism.

Although less descriptive, the risk statement can also be presented in a brief linguistic rating:

The risk of vandalism damage to the residential structure = "**very low**"

As the reader may have noticed, the terms used to rate these qualities can be imprecise. Moreover, verbal ratings provide no hard and fast rules for determining which combinations of ratings equal the various risk ratings. In cases where more precision is required, a seven-point verbal rating scale or numerical ratings on a 1 to 10 scale can be used. Numerical ratings – while more controversial – can provide more precise and more easily replicated assessments than can verbal ratings. The most common use, however is a hybrid in which analysts can benefit from the best parts of each.

In using a numerical system it is important to understand the theory behind the math. This mathematical theory provides the underpinnings for both the verbal and numerical systems for rating risks. The risk equation used in calculating these risks may be expressed as follows:

Risk = Loss Impact x (Threat x Vulnerability)

In this formula the "threat x vulnerability" segment represents the probability of the unwanted event occurring, and the "loss impact" represents the consequence of the loss of the asset to the asset owner.

Although the qualitative (numerical) approach is beneficial to the risk assessment process, its use requires additional discussion and training to be used properly. However, even with the basic

[5] Numerical risk ratings approaches are both beneficial and also useful under certain circumstances. However, their use is not covered here due to the space considerations.

qualitative approach, security professionals can, through practice and experience, develop a better understanding of the best ways to assess their own security analysis needs.

When the needs of the decision maker require only an assessment of risk to an asset, some analyses will end at this point. In most cases, however, the analyst will also be required to recommend countermeasures or other options for the decision maker to select from. In such cases, the following step is also included in the risk analyses.

Step 5. Identifying Countermeasures, Costs, and Trade-offs

The objective in analyzing countermeasures, costs, and trade-offs is to provide the decision maker with countermeasures, or groups of countermeasures, which will provide a range of protective values. Using the risk analysis worksheet as a guide, the experienced security professional will have little difficulty identifying what specific vulnerabilities need to be addressed. By evaluating the effectiveness of possible countermeasures against specific adversaries, the most cost effective ones should become apparent. For example, countermeasures, like access control, that protect against a variety of different unwanted events typically surface as the most cost-effective.

Regardless of whether the results will be delivered to the decision maker in writing or in a briefing, it is important to focus on both the risks and what should be done about them. Such presentations should make it clear that the end result of all this work is an educated decision on what to do next. To assist the decision maker in this task, the analyst should attempt to provide two or three countermeasure packages as options.

- The first of the countermeasure options should be the analyst's preferred option regardless of financial or political constraints. Although the decision maker may not ever select it, it provides a point of reference for the expenditures necessary to most effectively minimize the risk.
- The second option should be the countermeasure option which is most likely to be accepted, given the analyst's understanding of the decision maker's financial and political constraints.
- The third option should be the minimally acceptable option, which typically reflects the highest acceptable amount of risk.

Each of the options should also make clear the expected costs and amount of risks that would be accepted should the decision maker select it. This will effectively complete the risk analysis task and prepare the decision maker to make a *risk management decision.*

Using the Risk Analysis to Make Risk Management Decisions

Although the *risk management decision* is separate from the *risk analysis*, their relationship is so close that one cannot reasonably be discussed without the other. When decision makers choose a course of action based on a risk analysis, they are engaging in risk management. In many respects making the actual decision is the most difficult part of risk management. But, with a well documented risk analysis or briefing to support them, decision makers can decrease their reliance on intuition and opinion as the foundation for important decisions. Likewise, when unwanted events do occur, the decision maker can more easily defend these decisions through the use of the risk analysis, which provides documentation of all the relevant factors known at the time. As such, the risk analysis also provides a historical record of the careful consideration given to supporting the decision.

Although the risk analysis is not a binding document on the decision maker, it does provide an important communication vehicle for the analyst to provide expert judgment that the decision maker may not possess. Since only the decision maker can authorize funds for countermeasures, it is also their role to balance the amount of risk they will accept against cost and other constraints. Although decision makers need not act on all recommendations in an analysis, choosing not to do so is a decision for which they must also bear responsibility. Therefore, when serious or unacceptable risks exist which the decision maker does not possess the authority or financial resources to address, it is essential that the decision maker refer the issue to a higher level decision maker with the ability to address it.

Worksheet 4 – RISK ANALYSIS

Assets	Undesirable Events	Loss Impact Assessed as:	Threats Assessed as:	Vulnerability Assessed as:	Existing Countermeasures	Risk Assessed as:
People	Injury or death(s) due to violent crime	critical	low	medium	security awareness, door locks, ext. lighting	medium
	Injury or death due to natural disaster or accident	critical	low	low-medium	structural shelter, smoke detectors, first aid kit	low-medium
Residential Structure and Real Property	Damage or destruction due to hurricane/high winds	medium	very low	very low	structural shelter	low
	Flood damage/destruction	medium	medium	medium	property insurance with flood coverage	low
	Fire damage/destruction	medium	low	medium	smoke detectors, property insurance	low
	Vandalism damage	very low	low	medium	structural shelter, ext. lighting, property insurance	very low
Family Heirlooms and Photos	Loss or destruction by natural disaster, theft or vandalism	medium	low	medium	door locks, ext. lighting, smoke detectors, structural shelter	medium
Personal Property	Loss of property due to theft	low	medium	medium	security awareness, door locks, ext. lighting, property insurance	low
	Loss of property due to vandalism	low	low	medium	door locks, structural shelter, property insurance	low

Conclusion

The implementation of risk management in the government and contractor world presents many new challenges for security professionals. Adapting to a new reliance on research and analysis will require many to develop new job skills. Performing effective risk analyses will also require improvements in security's role in the collection, retention and dissemination of threat information. Finally, developing and improving writing and critical thinking skills will challenge even the best of security professionals.

Despite these challenges and the relative infancy of analytical risk management, risk-based decision making has already proven to be increasingly useful in reducing outdated and ineffective security policies and countermeasures. Conversely, risk assessments have supported decisions to enhance and fine tune security postures, better protecting U.S. national security and American lives in the process. An additional benefit of the process, according to some students, is that the process gives them a common professional language with other government and industry security professionals. Many also believe it will make it easier to "sell" their recommendations to their decision makers by educating them about the risks involved.

As can be expected with any new approach, there will be some growing pains as the clarification of roles and responsibilities within the process continues. As these are addressed by the Security Policy Board, the risk analysis is likely to become an increasingly useful tool for security professionals practicing risk management. It stands to reason that those security professionals who master the discipline early are likely to become increasingly valuable to the U.S. Government in its efforts to move risk management from theory to practice.

The author is the president and founder of Defensive Strategies Inc. and a Risk Management Trainer with Booz, Allen & Hamilton. Prior to founding Defensive Strategies, Mr. Jopeck was a security analyst with the Central Intelligence Agency, where he participated in the development of an community-wide risk management training program and conducted numerous risk analyses. The views expressed in this article are his own and do not necessarily represent the views of the US Government.

Downlink DoDSI presents the

Information Security Management Course

via video teletraining

The Information Security Team of the Department of Defense Security Institute (DoDSI) will broadcast the Information Security Management Course (ISMC) to classrooms across the United States on the following dates:

16 - 25 September 1997	(Eastern and Central Time Zones)
2 - 11 December 1997	(Mountain and Pacific Time Zones)
8 - 19 June 1998	(Eastern and Central Time Zones)
14 - 25 September 1998	(Mountain and Pacific Time Zones)

If your installation can receive a satellite training broadcast, (and it probably can) then you may want to subscribe to this training opportunity. Video teletraining is a highly cost-effective alternative to on-site, instructor-led training. If your training budget requires creative alternatives, video teletraining may be the solution. This training will be presented ***at no charge*** to the receiving activity.

The ISMC provides a comprehensive discussion of the DoD Information Security Program, to include the proper classification, downgrading and declassification of information, and safeguarding of classified information against unauthorized disclosure. Students will have the opportunity to discuss ideas, issues, problems and possible solutions with information security professionals. The course is designed for DoD military personnel and civilians with primary duty as a security manager within a DoD component information security program.

This resident course has been reengineered to be presented via interactive video teletraining. The course will be conducted over the Satellite Education Network (SEN) from its studios at Fort Lee, VA. Most military installations have the capability to take part in video teletraining. The SEN, 3.3 compressed digital system, is compatible with the Air Force Training Network, T-Net, and Warrior, and can be bridged to the Navy's C-Net.

The receiving site will have to provide an information security subject matter expert to help facilitate the course. The facilitator should have previously completed the resident ISMC and be available during course hours to assist the DoDSI faculty in conducting the course. The facilitator will be responsible for leading off-line activities such as practical exercises, quizzes and other administrative tasks.

If your government activity is interested in hosting or if you desire to attend this video teletraining course, call **Ray Yamaoka** at DSN 695-4893 or **Cheryl Cross** DSN 695-4890, Commercial (804) 279- extension for additional details.

Measuring Risk

BY RICHARDS J. HEUER, JR.
DEFENSE PERSONNEL SECURITY RESEARCH CENTER

Risk management is the process by which an organization identifies, reduces, and controls its potential risks and losses. Risks are identified and analyzed to determine the magnitude of the potential loss and the likelihood of such a loss actually happening. Countermeasures are analyzed to determine their cost and their effectiveness in lowering the probability of loss or in containing the amount of loss. Alternative countermeasures are identified and evaluated to select those which offer an optimal trade-off between risk reduction and cost.

In some respects, risk management is just a new name for what we have been doing all along. It's one of the current buzz words used by security management gurus. For the national security community, however, it symbolizes a dramatic change in the way we are expected to do our work, a change prompted by serious budget constraints and the end of the Cold War. Over the next 5 to 10 years, it is likely to transform the way we do business.

During the Cold War, we had a national commitment to do whatever it takes to win. Security was an absolute. No risk was acceptable. Security planning was driven by identification of threats and vulnerabilities, and every vulnerability had to be plugged. Programs were funded to achieve maximum effectiveness. With national survival at stake, almost any cost was permissible to ensure security. That has changed with the demise of Communism and identification of the budget deficit as a salient national problem.

Now, the goal is maximum efficiency in the allocation of limited resources. We are, for the first time, asking the question, "How secure is secure enough?" We are starting to define an "acceptable" level of risk, to look for the best *combination* of security and cost. The concept of acceptable risk is new in national security work, and it has broad ramifications.

Acceptable risk does not necessarily mean a level of risk with which we are happy, and it should certainly not mean simply ignoring risk. Less risk is always preferable to more risk if the cost and all other consequences are the same. In practice, however, cost in particular never is the same. A judgment about what level of risk is acceptable depends on what alternatives are available, and on analysis of the cost and risks associated with each alternative. Strictly speaking, therefore, one does not *accept* risks. One accepts an alternative that entails some identifiable level of risk among its consequences.

Risk management, in its simplest form, means making trade-off s between risk reduction and cost. It means doing a form of cost-benefit analysis. Although we can seldom put precise dollar values on all costs and benefits, we can and should approach problems from a cost-benefit perspective. We can identify program costs and analyze with as much precision as possible the incremental benefit (risk reduction) gained from the program. In this way, we can make a judgment backed by as much hard data as possible: Is the additional increment of risk reduction worth the cost? Are there alternative risk reduction measures that would provide, say, about 80% of the same benefits at roughly 40% of the cost?

We have seldom done this in the past. Programs were driven by an assessment of threat or vulnerability, e.g., Tempest, without too much regard for cost, as zero risk was the accepted goal.

The strongest evidence that we have not done much cost-benefit analysis is the unavailability of cost data on most activities and programs. Is information available on the full cost (including personnel costs) of an initial security clearance, a pe-

riodic reinvestigation, neighborhood check, polygraph, or the field inspection program, for example? It is not possible to do cost-benefit analysis without such cost data.

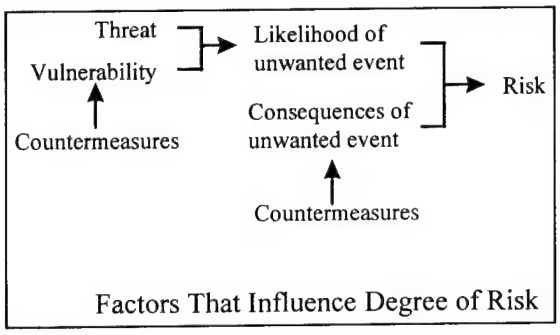
Similarly, program benefits have not always been fully identified and analyzed. For the personnel security program, for example, the benefit is often construed as simply reducing the risk of espionage. In practice, the greatest benefit may be the program's spillover impact on the quality of personnel in general. By screening out individuals with alcohol, drug, emotional, or financial problems or with a criminal history, the program reduces the incidence of many forms of counterproductive behavior — employee theft, employee violence, embezzlement, procurement fraud and sabotage, as well as performance deficiencies caused by substance abuse or emotional problems. Benefits of the personnel security program include stronger employee performance, fewer personnel problems, and lower employee turnover.

In its more advanced form, risk management involves making trade-offs between programs or program elements. It means optimizing the efficient or cost-effective allocation of limited resources among a menu of possible programs. This entails asking and answering questions such as the following: To optimize security within a fixed budget, should we spend X amount of money to achieve Y degree of risk reduction with program Z, or A amount of money to achieve B degree of risk reduction with program C? Such questions are difficult, as they require some common metric or standard for measuring different types of risks, e.g., comparing the benefits from reducing personnel security risk at cost A with benefits from reducing physical security risk at cost X.

Risk Assessment

The terms risk, threat and vulnerability are commonly used in a variety of ways. To forestall misunderstanding, it is useful to define how these terms are used and how they relate to each other in a risk management context. The relationships are pictured in the following graphic.

Risk is the potential for some unwanted event, such as loss of information or money, or harm to personnel or equipment. As shown in the graphic,



Factors That Influence Degree of Risk

risk is a function of the likelihood of the unwanted event occurring and the consequences if it does occur. The higher the probability and the greater the consequences, the greater the risk. Risk can be reduced by countermeasures that reduce the probability (i.e., reduce vulnerability) or limit the adverse consequences.

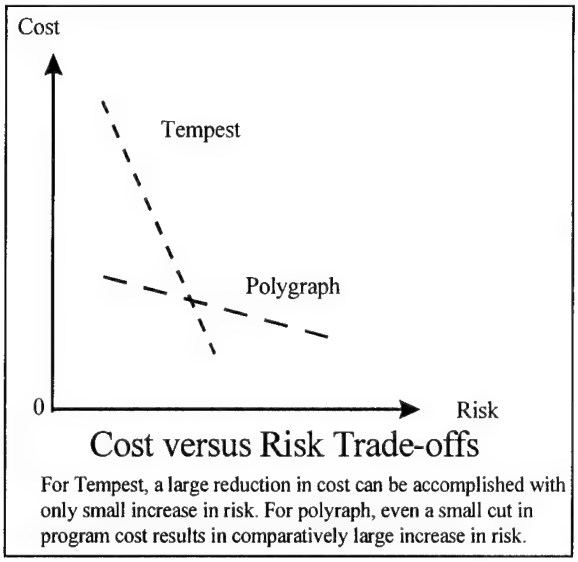
Likelihood of the unwanted event occurring depends upon threat and vulnerability. Threat is the capability and intention of an adversary to undertake actions that would be detrimental to U.S. interests. Threat is an attribute of the adversary only; it cannot be controlled by the U.S., although the adversary's intention to exploit his capability may be encouraged by U.S. vulnerability or discouraged by U.S. countermeasures

Vulnerability is any weakness that can be exploited by an adversary to cause damage to U.S. interests. The level of vulnerability, and hence level of risk, can be reduced by appropriate security countermeasures.

Consequences depend upon the nature of the loss and the nature of U.S. relations with the adversary at the time of the loss. For example, compromise of military plans will have far greater consequences if this occurs shortly before a military operation. Potential adverse consequences can be reduced by countermeasures such as effective compartmentation and access controls on computer systems.

Implementation of Risk Management

One starting point for implementation of risk management is to look at the relationship between cost and risk for each program or activity, and to consider the trade-off s between these two variables. Where can costs be cut the most with the



Cost versus Risk Trade-offs

For Tempest, a large reduction in cost can be accomplished with only small increase in risk. For polyraph, even a small cut in program cost results in comparatively large increase in risk.

least increase in risk? Where can a small increase in funding produce a significant reduction of risk? In short, where can limited resources – money and personnel – be deployed more efficiently.

The graphic on the next page presents a simplified illustration of two different relationships between cost and risk. It is the slope of the line that captures the essence of the relationship. The line labeled Tempest depicts a program where a large increase or decrease in funding would seem to cause a relatively small change in degree of risk. Such a program is a candidate for cost reduction, as large cost savings can be accomplished with a comparatively small increase in risk.

For the line labeled Polygraph, a relatively small increase or decrease in funding may translate into a relatively significant increase or decrease in risk. Even a small cut in program funding that required a reduction in polygraph use is shown, in this illustration, to cause a comparatively large increase in risk. One would not want to cut such a program, as the increased risk would be disproportionate to the money saved. One might even consider increased funding if the program is not already fully funded to the point of sharply diminishing returns.

The graphic is intended only to illustrate the principle of different trade-off s between cost and risk. It is not meant to be an accurate description of the actual Tempest or polygraph programs. If data were available to plot an accurate relationship between cost and risk for either of these programs, it would probably be a curved line rather than a straight line.

The box in the next column contains a suggested outline for what a full risk management analysis might look like.

Research Implications

Risk management requires hard data on the cost of whatever activity or program is being examined, as well as data to document risks (frequency and magnitude of loss events). Since we have in the past not done much of this type analysis, much of this information is not readily available.

Outline of Risk Management Analysis

I. Describe current situation
   - A. Describe current security countermeasures.
   - B. Describe risk these countermeasures are intended to protect against.
     1. Our vulnerability
     2. Threat (Who would want to exploit this vulnerability? What evidence is available of capability or intent to do so?)
     3. Consequences if unwanted event happens
   - C. Analyze effectiveness of these countermeasures in preventing unwanted events. (This is difficult, as one never knows what the losses would have been if countermeasures had not been in place.)
   - D. Analyze costs (including personnel, travel, overhead, and intrusion on privacy and civil liberties.)
   - E. Initial judgment: Are program costs proportionate to degree of benefit?

II. Identify alternative countermeasures.
   - A. Analyze the incremental change in cost and risk for each alternative countermeasure or set of countermeasures.

III. Identify optimal combination of risk reduction and cost.

Management cannot be responsive to costs unless it knows what the true costs are. Development of cost data for various programs and program elements would, itself, be a useful research project. These costs cut across the standard budget elements. For example, the cost of doing neighborhood checks or field inspections includes the cost of personnel, travel, and overhead. A full assessment of personnel costs might even include putting a dollar value on the present worth of future retirement annuity obligations.

For the risk side of the equation, we need to be certain we have an adequate process for collecting, storing and retrieving data on adverse security incidents – agent penetration, audio penetration of

various types of sites, physical intrusion in various types of sites, violence against employees, etc. We also need studies to identify and describe the financial, operational, political, public relations, legal, etc. costs of these security failures. This will give us some empirical basis for judging the frequency of such events and magnitude of loss, so that we can begin to relate the cost of security countermeasures to a realistic appraisal of risk.

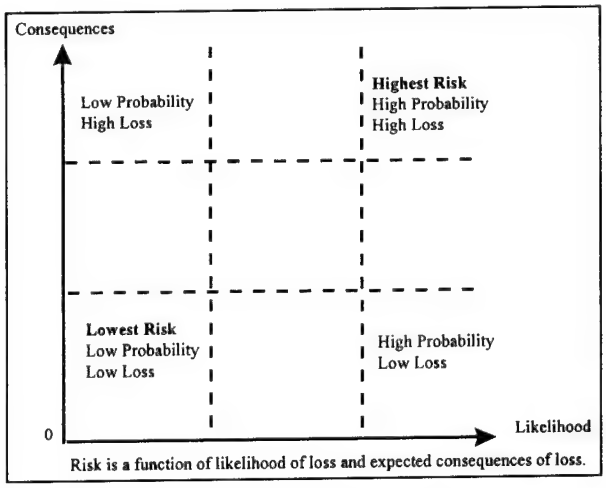
Risk management in the national security arena differs from risk management in many other fields, such as insurance, because of the difficulty we have in measuring security risk with any degree of precision. We generally cannot put a dollar value on the benefit of risk reduction, so there is no objective standard to determine what cost is justified to gain a given reduction of risk. That remains to be determined by policy judgment on a case-by-case basis.

It is possible, however, to compare degrees of risk. This is easiest when analyzing risks associated with alternative levels of funding for the same basic program or program element. When dealing with Tempest, for example, we know the threat is greater in some geographic areas than in others, and that vulnerability of systems depends upon distance to the nearest potential listening post. Based upon such variables, one can rank installations by risk and allocate funds in a manner that ensures maximum protection for any given level of funding. Such analysis provides decision makers with a sound basis for setting funding levels, which in effect defines how much protection to buy, or how safe is safe enough.

It is far more difficult to compare degrees of risk across different programs, e.g., to determine whether any given increment of funding is best invested in physical security or personnel security, or even in initial clearance investigation versus periodic reinvestigation. One can, however, approach such trade-off s across programs in a more systematic manner than has been done in the past. The key is to develop a system for categorizing levels or types of risk, so that one can at least rank order different risks on a common scale. One could then rank potential investments in security countermeasures according to their ability to reduce risk. This would not give specific quantitative values for comparing program costs with program benefits, but it would, at least, give a conceptual framework for making trade-offs between different types of programs to maximize risk reduction within the limits of available funding.

When ranking risks, several different dimensions of risk need to be considered. The most significant dimensions are the likelihood of the loss occurring and the consequences if it does occur. Other dimensions that may affect how one views the consequences are whether the loss is money, information or lives; whether the loss is short-term or long-term or even permanent; and the likelihood that countermeasures would actually be successful in reducing risk.

The graphic below shows a simple framework for assessing risk based on the likelihood of loss and consequences of loss. Any risk can be assigned



a position somewhere on this two-dimensional scale.

One possible approach is for a group of knowledgeable persons to make expert judgments about degrees of risk, and then to collate these multiple judgments into a single scale for comparing risks. This would facilitate trade-offs across program areas. Alternatively, a senior manager with supervision over all the relevant programs could make the trade-off judgments based on systematic analysis of costs and risks associated with each separate program.

Problems in the Perception of Risk

A persistent observation in psychological studies of how people perceive risk is that one's perception of risk is only loosely connected to the actual probability of an event happening. Psychologists have shown that two of the clues we use in judging the probability of some event are 1) the ease with which we can imagine relevant instances of the event, and 2) the number or frequency of such events that we can easily remember. We use these simplified rules of thumb when information is lacking or ambiguous concerning the true probability, as is so often the case. We are using them whenever we estimate frequency or probability on the basis of how easily we can recall or imagine instances of whatever it is we are trying to estimate.

Normally this works quite well. If one thing actually occurs more frequently and is more probable than another, we probably *will* be able to recall more instances of it. Events that *are* likely to occur generally *are* easier to imagine than less likely events. We are constantly making inferences based on these unconscious assumptions.

But we are often led astray, because the ease with which things come to mind is influenced by many factors, such as whether something has touched us emotionally, its vividness, and how recently we have been exposed to it, all of which may be unrelated to the correct probability. This is known as the *availability bias*, for our judgment is biased in favor of the probability of those events that are most readily available in our memory.

Consider two people who are smokers. One had a father who died of lung cancer. The other doesn't know anyone who ever died of lung cancer. Which one do you think perceives the highest risk associated with smoking? Should one's estimate of the probability of lung cancer be influenced by knowledge of a single case? How about two CIA officers, one of whom knew Ed Howard and the other who didn't know anyone who had ever turned out to be a spy? Which would be most concerned about personnel security risks?

Availability bias is most likely to influence judgments by policy makers and non-specialists who don't have the time or the information to go into the details. They must unconsciously take short cuts, and the normal short cut is the availability rule of thumb for making inferences about probability. Analysts who are studying all the data, rather than making quick and easy inferences based on imaginability, may be less influenced by availability bias.

Specialists in risk assessment have identified several other common errors that people make when judging risk.

- Overlooking the interrelationships between systems. For example, physical security systems that otherwise function effectively may be neutralized by a bad guard. One study of insider crime found that guards committed 41% of the crimes *against guarded targets*.
- Failure to consider the ways in which human error can affect technological systems. For example, alarm activations may be rationalized as harmless, or TV monitor screens may not be watched.
- Slowness in recognizing gradual, cumulative changes. For example, gradual changes in values and ethics in society as a whole may influence personnel security risk.

Conclusions

In the national security field, risk management is a new paradigm for making decisions on the allocation of security resources. It includes cost as a major variable in the decision calculus. Under risk management, the goal of security planning shifts from achieving maximum feasible security to achieving maximum efficiency in the allocation of limited security resources. Risk management requires rigorous analysis to identify risks, and to specify costs and benefits of alternative countermeasures to limit these risks. This analysis of risks, costs and benefits provides data on which to base judgments concerning the optimal trade-off between risk reduction and cost.

***

This article was originally written by Richards J. Heuer under contract with the Central Intelligence Agency and is reprinted by permission of the author.

Downlink DoDSI presents

Protecting Classified National Security Information

The Information Security Team of the Department of Defense Security Institute (DoDSI) will beam a **video teletraining course** to classrooms across the United States on the following dates:

1997	1998
30 September - 2 October	**27 - 29 January**
18 - 20 November	**28 - 30 April**
	25 - 27 August

If your installation has a satellite downlink (it probably does), then you can subscribe to this training opportunity. Video teletraining is a highly cost effective alternative to on-site, instructor-led training. If your training budget requires creative alternatives, video teletraining may be the solution. This training will be presented at no charge to the receiving activity.

The training will take place over three-days and was created specifically for television. It provides the **basic requirements** for personnel with routine access to classified information.

Students at your site will interact live with DoDSI instructors at Fort Lee, Virginia, via the Satellite Education Network (SEN) to learn the answers to these questions:

- What is classified information?
- Where does it come from?
- What's the correct way to

Mark it?	Handle it?
Process it?	Control it?
Store it?	Transmit it?
Destroy it?	

The students will learn the latest changes to the program and how they affect your organization. If your government activity is interested in hosting this video teletraining course, call **Cheryl Cross** at DSN 695-4390, commercial (804) 279-4390, for additional details.

Analytical Risk Management

A Systems Approach to Security Decisions

PREPARED BY THE CENTRAL INTELLIGENCE AGENCY, OFFICE OF FACILITIES AND SECURITY SERVICES

The Analytical Risk Management (ARM) Process

The task of protection has become increasingly complex with the rapid political, social, economic, and technological changes that are taking place today. At the same time, resources for security have become more constrained. The purpose of this guideline is to provide a systematic approach to acquiring and analyzing the information necessary to support decision makers[1] in the protection of assets and the allocation of security resources. It is designed as a tool to help security managers, analysts, and technicians in the day-to-day performance of their jobs – supporting the planning, implementation, and evaluation of risk-based security strategies.

Risk management is "the process of selecting and implementing countermeasures to achieve an acceptable level of risk at an acceptable cost." The analytical risk management process outlined in this guideline can be tailored and applied to any security analysis task. This document provides examples focused primarily on facilities, or site, protection and the assets contained within a facility or specified area. The process includes the following activities:

- Collection and evaluation of accurate and detailed information regarding the
  - nature and value of the assets
  - degree of a specific type of threat
  - extent of the related vulnerabilities
- Identification and evaluation of risks
- Cost-benefit analysis of countermeasures to mitigate specific, selected risks

These activities should be conducted on an ongoing basis in that risk management is a dynamic process requiring the monitoring of changes to asset value, threat, and vulnerability. Where significant risks have been accepted, it is important to include contingency planning as part of the risk management process.

The methodology uses a systematic approach in that it provides structure, record keeping, and objectivity within each step of the process. Each step outlined above is broken down further into substeps which are described in this guideline. Since risk analysis in not an exact science, it is important to maintain an audit trail that tracks the expert opinions and judgments made during each step. The documented audit trail can then be provided to the decision maker for review, and can be used as a baseline for follow-on or future analyses.

In conducting complex risk assessments, the effective application of this process integrates the skills, knowledge, and experience of a variety of specialists, as well as the customer and the security analyst. It is important for the analyst to know when and how to solicit information and advice from other professionals. Using a team approach helps ensure that the customer is provided with credible and defensible recommendations that are based on objectivity collected data, rather than on the judgment or memory of a single expert.

Risk management includes cost as a major variable in the decision making process. Identifying and prioritizing security requirements is especially important when resources are limited and can only be allocated against what we determine to be our most critical needs. With this model, the goal of security planning shifts from achieving maximum feasible security to achieving maximum efficiency in the allocation of limited resources.

[1] A decision maker is a person with the authority and resources to implement security countermeasures.

The five step process depicted below is an iterative versus sequential process. That is, each step may yield new information which affects the information developed earlier. Data gathered during each step of this process should be documented and maintained for further analysis and presentation to the customer as backup data for proposed recommendations and alternatives.

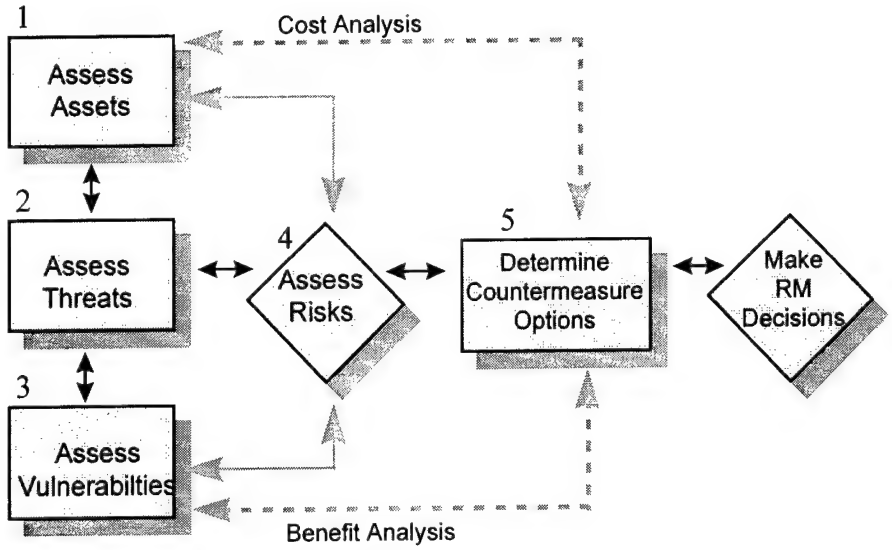


Figure 1 - Analytical Risk Management Process

"The process begins with an assessment of the value of assets, the degree of a specific threat, and extent of the vulnerabilities. These three factors determine risk. A decision is then made as to what level of risk can be accepted and which countermeasures should be applied. Such a decision involves a cost-benefit analysis, giving decision makers the ability to weigh varying security risk levels against the cost of specific countermeasures."
– quotation taken from: The Diplomatic Security Risk Management Policy

Outline of Analytical Risk Management Steps

STEP 1. Identify assets and loss impacts

1.1 Determine critical assets requiring protection.
1.2 Identify undesirable events and expected impacts.
1.3 Value/prioritize assets based on consequence of loss.

STEP 2. Identify an characterize the threat

2.1 Identify threat categories and potential adversaries.
2.2 Assess intent and motivation of adversary.
2.3 Assess capability of adversary or threat.
2.4 Determine frequency of threat-related incidents based on historical data.
2.5 Estimate degree of threat relative to each critical asset and undesirable events.

STEP 3. Identify and analyze vulnerabilities

3.1 Identify potential vulnerabilities related to specific assets or undesirable events.
3.2 Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities.
3.3 Estimate degree of vulnerability relative to each asset and threat.

STEP 4. Assess risk and determine priorities for asset protection

4.1 Estimate degree of impact relative to each critical asset
4.2 Estimate likelihood of attack by a potential adversary/threat.
4.3 Estimate likelihood that a specific vulnerability will be exploited.
4.4 Determine your relative degree of risk.
(expected impact (asset value) x (likelihood of successful attack (threat x vulnerability))
4.5 Prioritize risks based on integrated assessment.

STEP 5. Identify countermeasures, costs, and trade-offs

5.1 Identify potential countermeasures to reduce vulnerabilities.
5.2 Identify countermeasure capability and effectiveness.
5.3 Identify countermeasure costs.
5.4 Conduct countermeasure cost-benefit and trade-off analyses.
5.5 Prioritize options and prepare recommendation for decision maker.

Definition of Key Terms

For the purpose of this guideline, the following definitions of key terms should be used. The terms below are defined within the context of physical and operational security management and risk analysis within the Intelligence Community.

Risk Management: The process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

Risk: Risk is the potential for damage of loss of an asset. The level of risk is a combination of two factors:

1. The value placed on that asset by its owner and the consequence, impact, or adverse effect of loss or damage to that asset

2. The likelihood that a specific vulnerability will be exploited by a particular threat

Asset: An asset is any person, facility, material, information, or activity which has a positive value to the U.S. Government. The asset may have value to an adversary, as well as the U.S. Government, although the nature and magnitude of those values may differ.

Threat: Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage to, an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to U.S. interests. There are six primary sources of threats:

- foreign intelligence service
- insider
- criminal (outsider)
- terrorist
- environmental
- foreign military

Adversary: An adversary is an individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to the U.S. Government or its assets. These include intelligence services of the host nation or third party nations, politi-

cal or terrorist groups, criminals, and private interests.

Vulnerability: Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can result from, but are not limited to, the following:

- building characteristics
- equipment properties
- personal behavior
- locations of people
- equipment and buildings
- operational and personnel practices

Risk Assessment: Risk assessment is the process of evaluating threats to and vulnerabilities of an asset to give an expert opinion or calculation on the probability of loss or damage, and its *impact*, as a guide to taking action.

Impact: Impact is the amount of loss or damage that can be expected, as may be influenced by time or other factors.

Countermeasures: A Countermeasure is an action taken or a physical entity used to reduce or eliminate one or more vulnerabilities.

Cost Benefit Analysis: A cost-benefit analysis is the part of the management decision-making process in which the costs and benefits of each alternative are compared and the most appropriate alternative is selected.

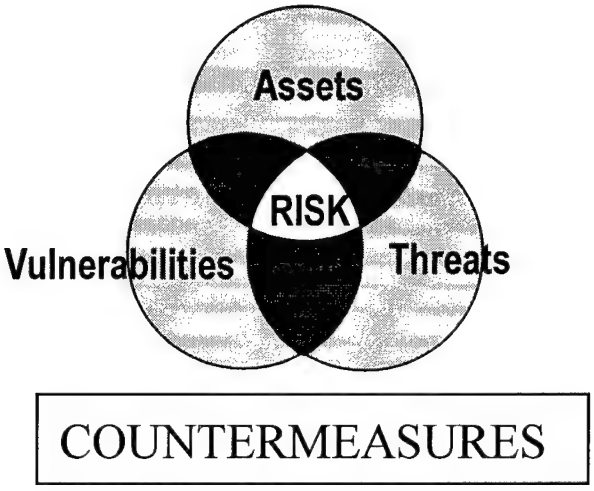
Costs include not only the cost of tangible materials, but also the on-going operations costs associated with countermeasure implementation. The cost of a possible countermeasure may be monetary, but may also include non-monetary costs such as reduced operational efficiency, adverse publicity, unfavorable working conditions, and political consequences.

Benefits are expressed in terms of the amount of risk reduction based on the overall effectiveness of the countermeasures with respect to the assessed vulnerabilities.

(Note: These definitions are consistent with the Overseas Security Policy Board's "Diplomatic Security Risk Management Policy.")

Training for Risk Management

BY AIMEE HUMMEL, BOOZ ALLEN & HAMILTON
CHAIR OF THE RISK MANAGEMENT TRAINING DEVELOPMENT TEAM



In today's rapidly changing world, the task of security protection has become increasingly complex. At the same time, resources for security have become more and more constrained. In 1995, the Central Intelligence Agency, working with the Defense and Intelligence Communities, developed a risk management methodology with the hope of intelligently balancing these competing demands. The result of this effort is a course to help security managers, analysts, and technicians in the day-to-day performance of their jobs—supporting the planning, implementation, and evaluation of risk-based security strategies.

Since August 1994, the Analytical Risk Project Team, which currently works under the Training and Professional Development Committee of the U.S. Security Policy Board, has been working hard to maintain the quality and reputation of its highly acclaimed Analytical Risk Management (ARM) course which was first offered in the fall of 1995. The work of the team (composed of government and contractor representatives from several organizations) is an example of effective interagency collaboration. The course was vetted by a broad range of contacts from within the CIA, NRO, the DCI Center for Security Evaluation, the National Security Agency, the DoD Security Institute, and the Interagency OPSEC Support Staff.

This future-orientated course encapsulates Intelligence Community efforts to manage more effectively security risks and demonstrates ways to maximize protection of facilities for the least cost. It is currently offered at a variety of training locations and is open to anyone with the appropriate need and qualifications as stated by each sponsoring organization. Three federal agencies currently sponsor a version of the original Analytical Risk Management Course developed under contract by Booz Allen & Hamilton presented under the auspices of the Central Intelligence Agency, Office of Facilities and Security Services.

Its first iteration in the fall of 1995 received rave reviews from the students, unusual for a new offering. It is now being presented by the CIA's Analysis and Policy Center (APC) once a month for CIA and Intelligence Community security officers. In addition, the Department of Defense Secu-

rity Institute and the Interagency OPSEC Support Staff have each offered a modified version of the course tailored primarily to the DoD community. Descriptions of all three course offerings and schedules for each follow on pages 29-31.

According to student feedback, the course has been successful in:

- Providing valuable assessment to managers who are responsible for accepting risks, planning, and funding security programs
- Defining consistent, replicable protection for various types of facilities
- Helping focus accountability for security decisions
- Adapting existing security documentation as input to the risk assessment framework
- Encouraging security officers to apply risk assessment methods in common sense ways that are not overly time-consuming and to integrate them into the management decision-making process

The analytical risk management process laid out in the ARM course, represents a major cultural and intellectual shift in the way the business of security is performed. Rather than simply establishing and enforcing rules, security officers are taught to provide expert advice to their customers and help them determine how best to apply available resources to protect their facilities, personnel, and information. Attendees learn to analyze data on assets, threats, vulnerabilities, and the costs of countermeasures alternatives, while employing a systems approach in their decision making. It is a systematic effort to teach security officers how to assess risks and formulate protective options.

The course has transformed vague procedures into practical ways of doing business. It is preparing officers to cope with rapidly changing circumstances that will require hard reviews of what to do and how much to spend to protect facilities. It makes clear to security officers that risk-taking is the rule, not the exception, and helps them distinguish between measured risks and poor risks. The course structure is flexible, accommodating a variety of case studies to ensure relevant training for all students.

In May, 1996, the Analytical Risk Management Course Development Team was awarded the National Intelligence Meritorious Unit Citation by the Director of Central Intelligence. The citation reads in part:

> *In recognition of its superior performance in designing a course that trains security officers to help their customers realistically assess security risks and maximize the protection of Intelligence Community facilities for the least cost. The course demonstrates concrete ways to define security threats and vulnerabilities, and employs systems analysis techniques to bring consistency to our security decisions.*

Risk Management for DoD Security Programs

hosted by the Department of Defense Security Institute

Course Description

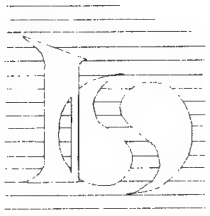
This course provides students with the appropriate background and skills to apply risk management principles and methodologies to the implementation of DoD security programs. It covers the fundamentals of risk management, asset assessment, vulnerability assessment, risk analysis, and the selection of cost-effective countermeasures. It additionally covers the functions, problems, and concerns of the risk manager and supporting personnel, their risk management responsibilities, and the development and implementation of a risk management program.

Target Audience:	Security managers and those involved in making risk management decisions regarding security countermeasures and safeguards
Prerequisite:	None
Course Length:	5 days
Location:	Department of Defense Security Institute, Richmond, Virginia
Clearance Required:	None
POCs:	Carl Roper, (804) 279-5593, DSN 695-5593 unclassified fax: (804) 279-5239 Mark Reardon, (804) 279-5170, DSN 695-5170 unclassified fax: (804) 279-6155

Course Schedule

December 15-19, 1997
January 26-30, 1998
February 23-27, 1998
March 30-April 3, 1998
June 1-5, 1998
August 3-7, 1998
August 31-September 4, 1998

Analytical Risk Management



hosted by the Interagency OPSEC Support Staff (IOSS)

Course Description

This course provides students with the appropriate background and skills to apply risk management principles and methodology to activities, operations, and security programs. It covers fundamentals of risk management, asset assessment, threat assessment, vulnerability assessment, risk analysis, and the selection of cost-effective countermeasures. It additionally covers the functions, problems and concerns of the risk manager and supporting personnel.

Target Audience:	Those involved in making risk management decisions, including managers and security personnel responsible for recommending or implementing countermeasures and safeguards.
Prerequisite:	None
Course Length:	4 days
Clearance Required:	U.S. Secret
POCs:	Lynne Clark, (301) 982-0720 unclassified fax: (301) 982-2913 Calvin Wood, (302) 982-0323 unclassified fax: (301) 982-2913 The IOSS tool free number is 1-800-688-6115 Push 3 when recording answers. Please be patient—there will be a short period of silence.

Course Schedule

March 2-5, 1998	Ft. Bragg, North Carolina
July 13-16, 1998	Kansas City, Missouri

Analytical Risk Management

A Systems Approach to Security Decisions

Hosted by the Central Intelligence Agency, Office of Facilities and Security Services

---

Course Description

This course provides a systems approach to security risk management when performing facility security activities related to the protection of people, information, activities, and property. It provides students with clear definitions of basic risk management terminology and a framework for obtaining and analyzing information to support risk-based decisions. Students participate in case study exercises that allow them to apply the risk management concepts presented in class. Given a scenario, students identify critical assets, threats, and vulnerabilities, estimate impacts of potential undesirable events, and determine site-specific, cost effective countermeasure options. It is a seminar and workshop-style course that requires a great deal of student interaction and teamwork.

Target Audience: The course is designed to help security and facilities managers, as well as their customers, in the planning, implementation, and evaluation of risk-based security strategies. The course is also highly relevant to counterintelligence and threat analysts working with the security community.

Prerequisite: None

Course Length: 4.5 days

Clearance Required: U.S. Secret

POCs: Alexis Scheffter, (703) 506-7176
unclassified fax: (703)938-4125
Aimee Hummel, (703) 506-7402
unclassified fax: (703) 506-7712

Course Schedule

September 15-19, 1997
October 6-10, 1997
January 26-30, 1998
February 16-20, 1998
April 27-May 1, 1998
June 15-19, 1998
August 3-7, 1998

New Independent Study Course from DoDSI

Basic Information Security DS 3121

- *Designed for* U.S. military and civilian personnel who need to understand the Information Security Program and its policies for classifying and declassifying information and who need to apply the policies to ensure that classified information is correctly identified and properly protected

- *Tracks* new revision of Information Security Program, DoD 5200.1-R

- *Replaces* Classification Management I and II (DS 3101 and 3102) and Protecting Classified Information I and II (DS 3103 and 3104)

- *Covers*:
  - -Basic Classification Management
  - -Duration of Classification
  - -Marking Classified Information
  - -Derivative Classification Issues
  - -Safekeeping and Storage
  - -Transmission and Transportation
  - -Disposal and Destruction

- *Enroll* by sending a completed DA Form 145 to:
  The Army Institute for Professional Development
  U.S. Army Training Support Center
  Newport News, VA 23628-9989

- *Include* $27.50 by one of the following:
  - -Money order, certified check, or company check payable to "Deputy Director for Finance."

  - -DD Form 1556, Request, Authorization, Agreement, Certification of Training and Reimbursement. In block 19a enter "Army Inst. for Professional Dev." In Block 19b enter
    U.S. Army Training Support Center
    Newport News, VA 23628-9989

  - -SF 1080, Voucher for Transfer of Funds. Funds should be transferred to the following address:
    USATSC
    ATTN: ATIC-RMB
    Bldg 1747
    Fort Eustis, VA 23604-5166

Army Correspondence Course Enrollment Application

DATE

For use of this form, see DA PAM 351-20: The proponent agency is TRADOC.

DATA REQUIRED BY THE PRIVACY ACT

AUTHORITY: 10 USC 3012 (B) AND (G).

PRINCIPAL PURPOSE: To obtain information necessary by Army schools to administer student participation in the Army Correspondence Course Program.

ROUTINE USES: Used by Army schools to obtain basic data needed to determine eligibility for enrollment, process applications, maintain student records, and perform all other administrative functions inherent in student administration.

DISCLOSURE: Mandatory. Failure to provide this informaiton could result in the applicant not being able to participate in the program.

*Submit one copy. See instructions on back page. Fill in all blocks (except **shaded blocks** which are for school use).*

1. Student SSN
2. Primary MOS/Duty MOS
3. CIV-SERIES
4. AOC Duty Position
5. ASI/SQI
6. Branch
7. DSN (telephone)
COMM (telephone)
8. Group Number
9. Rank/Civ Grade
10. Component Code
11. RYE Date Day
Month (abbreviate)
Year
12. School Code
13. Enrollment Code
14. Phase
15. Course Number
16. Rep Qty
17. Unit Identification Code
18. Subcourse Exemption

19. I REQUEST ENROLLMENT IN: (Course Title, MOS if applicable or subcourses desired).
(Do not list individual subcourses if you are enrolling in a course).

NOTE: If you were previously enrolled in this course, indicate date of termination of enrollment. _____

Are you currently enrolled in the ACCP? _____ YES _____ NO

20. MAIL TO:

The Army Institute for Professional Development
U.S. Army Training Support Center
Newport News, VA 23628-9989

THRU: (Unit to which assigned)

21. Title of approving official

Unit Address Line 1 Unit Designation (May not be left blank.)

Unit Address Line 2 P.O. Box or Street (May be left blank.)

Unit Address Line 3 City, Post or APO/FPO

State or AE/AP/AA

Zip + 4

FROM: (Mailing address to which subcourses are to be sent)

22. Last Name
First Name
Middle Initial

Student Address Line 1 Unit Designation or P.O. Box or Street (May not be left blank.)

Student Address Line 2 P.O. Box or Street (if not given on Student Address, Line 1)

Student Address Line 3 City, Post, or APO/FPO

State or AE/AP/AA

Zip + 4

23. **ARMY SCHOOL COURSES AND CORRESPONDENCE COURSES COMPLETED**

SCHOOL	TITLES OF RESIDENT OR NONRESIDENT COURSES OR INDIVIDUAL SUBCOURSES COMPLETED	DATES

The Commander will verify the above from personnel records or soldier's individual records.

24. I have reviewed DA PAM 351-20, and understand the eligibility requirements that I must maintain to sustain my enrollment in this course. I further understand that assistance is not authorized when completing subcourse test.

Signature of Applicant _____

25. I have reviewed the course objectives and prerequisite enrollment requirements in DA PAM 351-20 and determined the applicant is eligible for enrollment in this course.

Unit Cdr or other approving officer
Name (printed or typed) _____ Date _____

Signature _____

DA PAM 351-20 contains information pertaining to enrollment qualifications, submission of application, and courses available.

INSTRUCTIONS TO APPLICANT

Complete by legibly printing only in areas that are not shaded. The shaded areas are used for data entry. Enter only one character per block (example below).

1. Student SSN

2	4	4	3	2	0	1	6	4

9. Rank/Civ Grade

S	G	T	M	A	J

ITEM 1. SSN Foreign students must leave blank.
ITEM 2. Student's PMOS (Primary MOS) and DMOS (Duty MOS). Enter numeric and alpha identifiers.
ITEM 3. Civ-Series number (for example 1702)
ITEM 4. AOC Area of Concentration or Duty Position. Submit information required to qualify for enrollment.
ITEM 9. RANK: RA warrant officers and enlisted personnel who hold a reserve commission and are enrolling in officer career development courses must enroll in their reserve capacity.
ITEM 10. Component Code: Student categories: Enter one of the following as appropriate:

02	Active Duty	09	USAR ENL	15	FGN CIV	20	CADET
03	RA/AUS ENL	10	NGUS ENL	16	USAF	31	IRR (OFF)
06	RET MILITARY	12	NDCC/ROTC/JR	17	USN	32	IRR (ENL)
07	USAR OFF/WO	13	FGN MIL	18	USCG	33	NAF (VOL)
08	NGUS OFF/WO	14	U.S. CIV	19	USMC		

ITEM 11. RYE Date (Retirement Year Ending Date): USAR and NG applicants not on active duty must enter the anniversary date of their retirement year ending day and month.

Where to mail application: See block 20.

Revised DoD Directive 5200.1 and DoD Regulation 5200.1-R

Earlier this year the Office of he Assistant Secretary of Defense, Command, Control, Communications and Intelligence issued a revised DoD Directive 5200.1 and DoD Regulation 5200.1-R which govern the Department of Defense Information Security Program. Both documents are available in hard copy through regular publication and by way of the Internet at the DoD Security Institute's home page (http://www.dtic.mil/dodsi).

As stated by Mr. J. William Leonard, Director of Security Programs, the purpose of the revision is to implement within the DoD the provisions of Executive Order 12958 and the Office of Management and Budget/Information Security Oversight Office Implementing Directive. The revisions also accommodate the safeguarding and policy guidance expected to be issued through the Security Policy Board structure. A summary of changes to the directive and regulation follow. The staff point of contact for these changes is Mr. William H. Bell, e-mail: bellw@osd.pentagon.mil .

Summary of Changes

Directive

- Language is added to indicate that ASD(C3I) is responsible for assisting USD(Acquisition and Technology), as required, in implementing the DoD Acquisition Systems Protection Program.
- Responsibility for oversight of the Information Security Program is split between the Assistant Secretary of Defense (Command, Control and Intelligence) and the Under Secretary of Defense (Policy). USD(P) is responsible for Special Access Programs, foreign government information (including NATO), National Disclosure Policy, and security for international programs.

Regulation

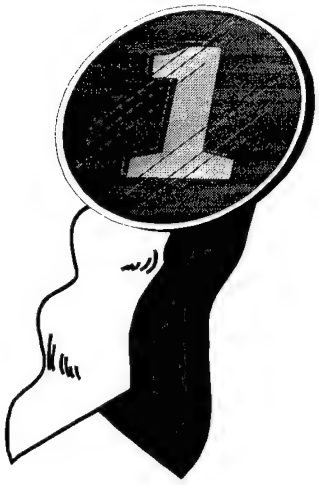
Classification/Downgrading/Declassification

- Information will normally be classified for 10 years. Specific action is required to extend classification.
- The Originating Agency's Determination Required (OADR) declassification instruction is eliminated.
- Information 25 years old and older that has permanent historical value will be declassified automatically unless an agency takes specific action to extend classification.
- To be exempted from 25-year declassification, information must fall into one of the specific exempted file series identified by the Secretary of Defense and Secretaries of the Military Departments, or it may be exempted by the Secretary of Defense or a Secretary of a Military Department if it falls into one of nine narrowly defined areas for exemption stated in the Regulation. Subsequent exemptions must be approved by the Interagency Security Classification Appeals Panel.
- More detailed document marking is required. Original classifiers must be identified by position title or by a specific personal identifier, and a concise reason given for classification. A "Classified By" marking or a "Derived From" marking must be used to better differentiate between originally classified documents and those that are derivatively classified.
- Original classifiers are required to receive training on the classification process and responsibilities.
- The regulation increases personal accountability for the management of classification. Classification management is added as a critical element for review during evaluations of supervisors and employees.
- A new process is established for classification challenges, self-inspection programs, and oversight of special access programs.

Safeguarding

- NATO information is to be safeguarded in accordance with USSAN 1-69. Other foreign government information is subject to the provisions of the Regulation except as specified in treaties or international agreements.
- The authority of military commanders to modify provisions of the Regulation to meet operational requirements is expanded to include not only combat operations but also peacekeeping, and other operations involving military deployments.
- Accountability; e.g., records of receipt, disposition, access, inventory; for any level of classified information, including TOP SECRET, is required only when technical, physical and personnel controls are insufficient to deter or detect access by unauthorized persons.
- The Defense Courier Service (DCS) is authorized to use a specialized shipping container for the movement of DCS qualified material on direct flights in lieu of an escort, provided the container is of sufficient construction to provide evidence of forced entry and is equipped with a high security padlock and electronic sensor to provide evidence of surreptitious entry.
- General Services Administration (GSA)-contract carrier (currently FedEx) is authorized for the transmission of SECRET and CONFIDENTIAL material within the U.S. and its territories. This applies only to U.S. Government activities, not contractors. [The use of this option for contractors will be addressed through the National Industrial Security Operating Manual (NISPOM) process.]
- Authority is delegated to Heads of DoD components to approve classified meetings.
- The Regulation clarifies the use of DD Form 2501, "Courier Authorization."
- The Regulation establishes minimum requirements. Senior agency officials may, through issuance of appropriate component guidelines, approve the use of alternative or compensatory security controls. Such approval must be documented and furnished upon request to other agencies with whom classified information or security facilities are shared.
- Authority to use certain security controls (lists or rosters, unclassified nicknames requiring that material be placed in specially marked envelopes and stored separately, and unique oversight or inspection procedures) requires approval by an Original Classification Authority. Central records must be maintained.
- Security controls unique to Special Access Programs are delineated:
  - ⇒ More stringent personnel security investigative or adjudicative requirements than those normally required for a comparable level of classified information
  - ⇒ The use of specialized non-disclosure agreements/briefing forms
  - ⇒ Use of any special terminology, other than a nickname, as prescribed for the handling of special message traffic, or special marking, to identify or control dissemination of information
  - ⇒ Exclusion of a classified contract from inspection by the Defense Investigative Service
  - ⇒ Use of a centralized billet system to control number of personnel authorized access
- Detailed guidance is provided on topics to be covered during an initial, continuing education/refresher training for original and derivative classifiers, declassification authorities, security management, and other personnel.
- Guidance issued by the DCI (DCID 1/7) regarding the elimination of NOFORN, NOCONTRACT and WINTEL is incorporated as an Appendix. (This guidance will be provided to Components when it becomes available.)
- An appendix is added on controlled unclassified information. It provides security personnel with the essence of existing established guidance relating to information that, while unclassified, requires some degree of protection.

Attention Security Educators, here's your chance to sign up for the:



Train-the-Trainer/Security Briefers Courses!

offered at the DoD Security Institute
in Richmond, Virginia, on:

Train-the-Trainer	Security Briefers Course
June 23-27, 1997	June 25-27, 1997
September 8-12, 1997	September 10-12, 1997
January 26-30, 1998	January 28-30, 1998
April 13-17, 1998	April 15-17, 1998
July 20-24, 1998	July 22-24, 1998

If interested in attending any of the above classes, please mail or fax us the Registration Form on the reverse. The fax is (804) 279-6406, DSN 695-6406. Address is DoD Security Institute, Attn: Registrar, 8000 Jefferson Davis Hwy, Richmond, VA 23297-5091.

If you'd like to *host* these courses, call Linda Braxton at (804) 279-6076, DSN 695-6076. If you have any questions about the courses, call Linda Braxton or Gussie Scardina, course instructor, at (804) 279-5308, DSN 695-5308.

About the courses:

The **Security Briefers Course** (SBC) prepares security professionals to plan and deliver effective security briefings. Activities include preparing a briefing plan; presenting a briefing in a clear and interesting manner; designing and using briefing aids; and evaluating the effectiveness of an oral briefing.

The **Train-the-Trainer** for the SBC prepares security specialists to *teach* the Briefers Course. It begins as a two-day instructor preparation workshop before the first day of the SBC. The next three days are spent *teaching* the SBC under the supervision of DoDSI staff. Graduates return to their organization with instructor guide, student workbook, and handout packet. Activities include using the SBC materials, teaching the lessons in the SBC, assisting others to prepare briefing plans, and facilitating practice briefing sessions.

DoD Security Institute
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, Virginia 23297-5091

Registration Request

Please print or type, and fill in all *applicable* information. In addition to serving as a permanent record of your registration, a class roster will be compiled prior to class from the information on this form. The roster will include your name, position, address, and phone number. If you have objections to this, please let us know. If you have any questions, call the Registrar (804) 279-4758/4892, DSN 695-4758/4892 (FAX 6406).

Privacy Act Statement

Authority: 5 USC 301 and DoD Directive 5105.42.

Principal Purpose or Purposes: The primary purpose served by DSI Form 2021A is to serve as a permanent enrollment record. Social security number (SSN) is required to distinguish between records of students with the same name.

Routine Uses: DSI Form 2021A is routinely used as an alphabetical index and locator card for students and as a course completion record.

Disclosure: Disclosure of information, including SSN, is voluntary. Failure to provide such information could result in inaccurate records of students with same name.

Course title	Course no.	Course dates

Social Security Number	Name (Last)	(First)	(MI)	(subtitle: Jr., III, etc.)

(Mr./Mrs./Ms.) Rank/Rate	Position	Mil/GS Grade

Agency/Activity Code	Birth date MM/DD/YY	Gender (circle) F M	Clearance level (circle) C S TS None

Duty station/Facility address	Job Title/Name/Address of Supervisor (if same address ❐)
(city) (state) (zip)	

DSN: _____ DSN: _____

Commercial No. _____ Commercial No. _____

Fax: _____ Fax: _____

E-mail address: _____ E-mail address: _____

Agency/Activity: (If your agency is not listed, please write it out.)

DAF	Air Force	DJT	Joint Command	OFE	Federal Emergency Mgmt. Agcy.
DAY	Army	DMC	Marine Corps	OFG	Foreign Govenment
DSA	Defense Info. Systems Agency	DNY	Navy	OJU	Justice Department
DIA	Defense Intelligence Agency	DSD	Secretary of Defense	ONR	Nuclear Regulatory Commission
DIS	Defense Investigative Service	DoD	Other Department of Defense	OST	State Department
DLA	Defense Logistics Agency	OED	Education Department	OTP	Transportation Department
DMA	Defense Mapping Agency	OEG	Energy Department	OCP	U.S. Capitol Police
DNA	Defense Nuclear Agency	OEP	Environ. Protection Agcy.	IND	Private Industry

Education Level: High School, Associate, Bachelor, Masters, PhD, JD, Some College

Regional OPSEC Symposium

November 18-20, 1997 in San Antonio, Texas
December 2-4, 1997 in Richmond, Virginia

About the symposium

Each symposium brings training and professional development assistance to OPSEC practitioners throughout federal government and industry. The symposia are comprised of classified and unclassified sessions. Unclassified sessions include training sessions, briefings, and workshops. Classified sessions are one-hour briefings on threat and related topics; transportation to the classified sessions will be provided from the hotel. The one-day OPSEC Fundamentals Course is open to anyone requiring introductory training. The one-day seminar on OPSEC Assessments has as a prerequisite either an introductory course or 1 year experience. Technical sessions are one-hour briefings by experts on subjects directly related to the practice of OPSEC. Workshops offer participants an opportunity to participate in a new approach or work with experienced practitioners. Each symposium will be a duplicate of the other in structure and subject matter.

Who should attend

Anyone involved in OPSEC, Information Warfare, or Risk Management will find useful training, interesting presentations and activities, and excellent opportunities to network with other practitioners.

Schedule

Monday, 2:00 p.m. - 5:00 p.m.
Registration

Tuesday, 7:00 a.m. - 4:30 p.m.
Registration
Introduction to OPSEC Course
(prerequisite: none)
OPSEC Assessments Seminar
(prerequisite: basic course or 1 year experience)

Wednesday, 7:00 a.m. - 5:00 p.m.
Registration
Exhibition
Briefings
Workshops
Round Table

Thursday, 8:00 a.m. - noon
Classified sessions
U.S. Secret clearance required

Sessions

Introduction to OPSEC Course
OPSEC Assessments Seminar
The Economic Espionage Act
Collection Trends in the U.S. Defense Industry
Open Source, Commercial Imagery, & OPSEC
OPSEC Program Development
Developing and Using an Adversary Strategy

Exhibits

The Federal Business Council will sponsor an exhibition from 10:00 a.m. to 2:00 p.m. on Wednesday (Nov. 19 and Dec. 3). Exhibits cover OPSEC, Risk Management, Security, Communications, and Threat Research & Assessment. No charge. Exhibitors call 1-800-878-2940, ext. 201.

Registration and Fees

Return registration form to OPS, 9200 Centerway Road, Gaithersburg, MD 20879 or FAX to (301) 840-8502.

	Course	Symposium	Both
OPS member	$ 60	$ 95	$140
non-member	$ 70	$115	$165

Registrants attending classified sessions must pass SECRET clearances no later than 10 days prior to each symposium.
Nov. 18-20. FAX the security form to (210) 977-3125.
Dec. 2-4. FAX the security form to (804) 279-5239.
Be prepared to provide the original at registration.

Accommodations

Call the hotel for reservations. For special rate, mention the Regional OPSEC Symposium.
San Antonio: Radisson Market Square, (210) 224-7155. $63 for government personnel; $79 for non-government.
Richmond: Holiday Inn Select, (804) 379-3800. Government per diem rate for all participants.

For more information

Interagency OPSEC Security Staff, (301) 982-0323
OPSEC Professionals Society, (301) 840-6770

Sponsored by the Interagency OPSEC Support Staff and the OPSEC Professionals Society

REGIONAL OPSEC SYMPOSIUM
Security Form

There will be no provision for security clearance certification on site.

Please indicate if you are registering for:

San Antonio, TX ◆ November 18-20 ☐

Richmond, VA ◆ December 2-4 ☐

Name		
Please complete one of the following: Rank and Service	Company	
Business address		
Phone	FAX	E-mail
Date and Place of Birth		
Social Security Number		
Signature		

The following to be completed by Security Officer

Issuing agency	Date issued
Security Officer name	
Phone	
Security Officer signature	Date

WHERE TO SEND THIS FORM:

San Antonio: FAX to (210) 977-3125, Attn: Mr. Len Thomas

Richmond: FAX to (804) 279-5239, Attn: Mr. Pat Nemanic

REGIONAL OPSEC SYMPOSIUM Registration Form

Please indicate if you are registering for:

Regional OPSEC Symposium ◆ November 18-20, 1997 ◆ San Antonio, TX ☐

Regional OPSEC Symposium ◆ December 2-4, 1997 ◆ Richmond, VA ☐

Send to: OPSEC Professionals Society, 9200 Centerway Road, Gaithersburg, MD 20879
or FAX (301) 840-8502

Please complete one form per person attending. A networking list will be provided at registration.
If you wish to have your information withheld from the networking list, please check here. ☐

Name: _____ Organization/Company: _____

Address: _____

Commercial phone (no DSN): _____ FAX: _____

E-mail: _____

How would you like your name to appear on your badge?

_____

How would you like your organization to appear on your badge? ___ as above ___ none

other _____

IF YOU ARE REGISTERING FOR TRAINING, please indicate which course you wish to attend.	
Introduction to OPSEC	OPSEC Assessments (prerequisite: Basic OPSEC Course or 1 year experience)

PLEASE CIRCLE APPROPRIATE FEE

	Course only	Symposium only	Course & Symposium
OPS member	$60	$95	$140
Non-member	$70	$115	$165

Fees include sessions, proceedings, breaks, and lunch on the first day during training.

Amount enclosed: _____ DD 1556 or SF 182 enclosed

Payment may be made by check, money order, government training form, VISA, MasterCard or American Express. Make checks and money orders payable to ***OPSEC Professionals Society***. You may FAX a copy of the training form with your registration form.

Credit card payment: VISA MasterCard American Express

Card number _____ Expiration date: _____

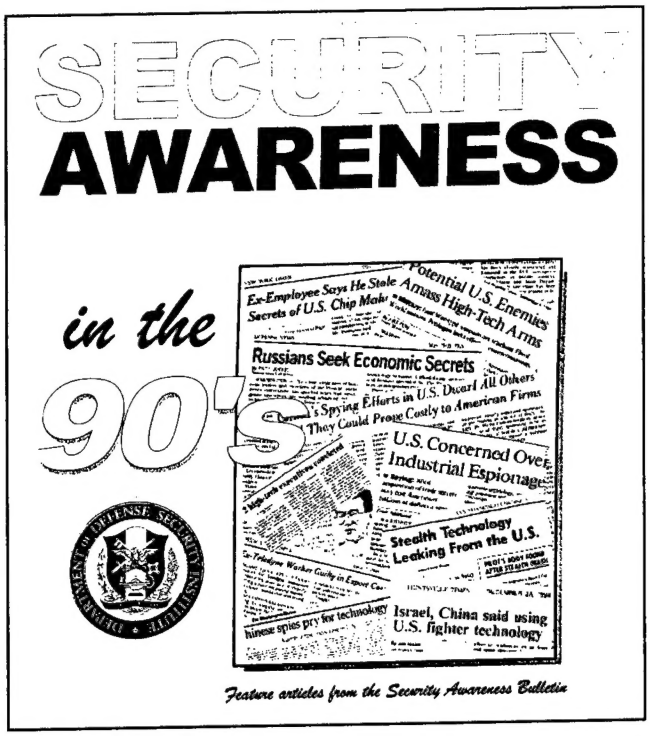
Card owner name: _____ Signature: _____

Security Awareness in the 1990s

feature articles from the
Security Awareness Bulletin 1990-1996

Subject areas:

- the foreign intelligence threat
- espionage case studies
- industrial security
- information systems security
- security policy and programs
- the threat to U.S. industry



This is the second compilation of past *Bulletin* articles issued by the DoD Security Institute. The first volume, Security Awareness in the 1980s, was published in 1990 and was an immediate success. The new edition picks up where the former left off. It will be particularly useful to younger security professionals who didn't see these articles when they first appeared.

.....

Superintendent of Documents **Publication** Order Form

Order Processing Code
*8012

___ copies of **Security Awareness in the 1990s,** S/N 008-047-00409-5 at $22.00 each ($27.50 foreign).

The total cost of my order is $ _____. Price includes regular shipping and handling and is subject to change.

Name or title (Please type or print)

Company name Room, floor, suite

Street address

City State Zip +4

Daytime phone including area code

Purchase order number (optional)

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐—☐

☐ Visa ☐ MasterCard

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

(expiration date)

☐☐☐☐

Thank you for your order!

Authorizing signature

Mail to: Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Security Awareness Bulletin

Subscription Service

As we announced in our last issue, beginning with the first quarter of 1997, the *Security Awareness Bulletin* can no longer be distributed free of charge to Defense contractors and to non-Defense agencies.

But the good news is that anyone can get the *Bulletin* one of two ways:

1. By accessing our DoDSI web page (http://www.dtic.mil/dodsi). We will send you an automatic e-mail notice via the Internet when a new issue goes on-line. Just enter your e-mail address on the registration form for this service in the *Security Awareness Bulletin* section of our web page.

2. By signing up for a low-cost subscription service that we have arranged through the U.S. Superintendent of Documents.

Here's how the Bulletin Subscription Service works: Send in a copy of the form below with a check for the appropriate amount and you will receive the *Bulletin* four times a year.

United States Government
INFORMATION

Order Processing Code
*5769

Credit card orders are welcome!

Fax your orders (202) 512-2250
Phone your orders (202) 512-1800

Security Awareness Bulletin at $9.00 ($11.25 foreign) per year (four issues)
The total cost of my order is $ _____.

☐ YES, please send _____ subscription(s) to:

_____
Name or title (Please type or print)

_____
Company name Room, floor, suite

_____
Street address

_____
City State Zip +4

_____
Daytime phone including area code

_____
Purchase order number (optional)

For privacy protection, check the box below:

☐ Do not make my name available to other mailers

Check method of payment:

☐ Check payable to: Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐—☐

☐ Visa ☐ MasterCard

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

(expiration date)

☐☐☐☐

_____
Authorizing signature

Mail to:
Superintendent of Documents, PO Box 371954, Pittsburgh PA 15250-7954

Important: Please include this completed order form with your remittance. *Thank you for your order!*

Security Awareness Publications Available from the Institute

Publications are free. Just check the titles you want and send this form to us with your

address label

Our address is:

DoD Security Institute
Attn: Security Education & Awareness Team
8000 Jefferson Davis Hwy, Bldg 33E
Richmond, VA 23297-5091
(804) 279-4223 or DSN 695-4223;
FAX (804) 279-6406, DSN 695-6406
e-mail gulledget@dodsi.dscr.dla.mil

❑ **Recent Espionage Cases: Summaries and Sources**. July 1997. Ninety-three cases, 1975 through 1996. "Thumb-nail" summaries and open-source citations.

❑ **Announcement of Products and Resources**. October 1996. A catalog of security education videos, publications, posters, and more you can order.

❑ **DELIVER!** Easy-to-follow pamphlet on how to transmit and transport your classified materials. Written specifically for the Department of Defense employee. February 1997.

❑ **Terminator VIII**. Requirements for destruction of classified materials. Written specifically for the Department of Defense employee. September 1992.

❑ **STU-III Handbook for Industry**. To assist FSOs of cleared defense contractors who require the STU-III, Type 1 unit. Covers step-by-step what you need to know and do to make the STU-III a valuable addition to your facility's operations.

❑ **Survival Handbook**. The basic security procedures necessary for keeping you out of trouble. Written specifically for the Department of Defense employee. March 1997.

❑ **Layman's Guide to Security**. The basic security procedures that you should be aware of when handling classified materials in your work environment. March 1997.

❑ **Acronyms and Abbreviations**. Twelve pages of security-related acronyms and abbreviations and basic security forms. October 1995.

❑ **Take A Security Break.** Questions and answers on security and other topics.

❑ **Take Another Security Break.** More questions and answers.

❑ **Take A Third Security Break**. More questions and answers.

❑ **Lock Up!** A pamphlet on the structural standards and other security requirements for the storage of conventional arms, ammunition, and explosives. August 1995.

*U.S. Government Printing Office: 1997 — 527-109/60004